UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 03/24/2011
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
03/24/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/752,420	ROSE ET AL.	
	Examiner	Art Unit	
	Cordelia Zecher	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 14, 2011 has been entered.

Response to Arguments

2. Applicant's arguments filed March 14, 2011 have been fully considered but they are not persuasive.

3. Applicant argues that the examiner has failed to characterize a particular device between source system 1, destination system 2, and central system 5, of Arthan, as corresponding to the claimed “single device”. To clarify the examiners position, the central system in combination with the source system, teaches that claimed “single device”. As explained in Arthan, the source and destination system may be complex distributed systems and may comprise a large number of physically separate nodes (column 2, lines 30-34). Accordingly, an ordinary skilled artisan would have understood that the central system may be a node of the distributed source system and, therefore, a single device.

4. In addition, it is the Examiner's position that absent evidence of new or unexpected results, a modification decreasing the pieces of hardware (*e.g.* having one piece of hardware perform a task previously performed by two) is analogous to making functions, structures, or actions integral. It is the Examiner's position that when the difference between the claimed invention and the prior art is that the prior art does not disclose an element as integral, as a matter of law, it would have been obvious to one having ordinary skill in the art to make the element integral. See MPEP §2144.04 V. *B.* and *In re Larson*, 340 F.2d 965, 968, 144 USPQ 347, 349 (CCPA 1965). It is desirable to have one device perform the functions previously performed by two to minimize the amount of hardware required.

5. Applicant argues that none of the devices of Arthan includes a storage medium to store the first private key and a transmitter to output the second private key such that it is not stored in the storage medium, and a processor that uses the stored first private key for authentication prior to using the second private key. However, Arthan teaches that the source system stores the private key in memory (column 2, lines 48-50), and that there is a private key and a spare private key, the spare private key not being put into use until the private key is compromised (column 4, lines 15-23). Therefore Arthan teaches storing the first private key wherein the processor uses the stored first private key for authentication prior to using the second private key.

6. While Arthan does not explicitly disclose that the second private key is actually transmitted, Kurn teaches that the protection key is divided into shares and shared with the owners (paragraph 89), and once the shares are sent that the key is erased from

memory (paragraph 102). Therefore Kurn teaches a transmitter to output the second private key such that it is not stored in the storage medium.

7. Applicant argues that the combination of Arthan in view of Kurn would result in a complete failure of Arthan. However, Arthan teaches that the spare key needs to be held securely after generation and then called up when required (column 4, lines 30-32). Therefore combining Arthan in view of Kurn would not result in a failure of Arthan but rather increase the security since the spare key would be completely secure since no one party or device has access to the key.

8. Applicant argues that one of ordinary skill in the art would be motivated not to combine Kurn with Arthan. However, as explained above, one of ordinary skill in the art would be motivated to combine the teaches because Arthan requires the spare key to be secure (column 4, lines 30-32) and Kurn teaches keeping the key secure in that no one individual can produce the key (paragraph 27).

9. Applicant goes on to argue that the independent claims rejected over Arthan in view of Kurn in view of Hansmann, and corresponding dependent claims are allowable for similar reasons. However, for the reasons explained above, all of the claims are still rejected.

10. Applicant argues that Arthan fail to teach re-creating a second private key at a mobile user device that has no access to a first private key. Applicant argues that the teaching of Arthan that the spare key is used when the current key is compromised (column 4, lines 15-22) is not equivalent to not having access to the private key. While Arthan does teach that the compromised key could include a key that has been cracked

(column 5, lines 30-35), Arthan does not exclude a scenario when the compromise could include the key being not accessible to the device. A compromised key can include a key that is lost. This is evidenced by Asay et al's US Patent 5,903,882. Asay teaches that compromised keys include both lost and stolen keys (column 2, lines 61-64). Therefore the compromised key of Arthan includes keys which are not accessible to the system.

11. Applicant's arguments with respect to claims 57 – 68 with regards to outputting the third private key while retaining a second private key have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

12. Claims 50, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan et al's US Patent 6,782,103 B1, and in view of Kurn et al's US Publication 2002/0071561 A1.

13. Referring to claim 50, Arthan teaches:

a. A processor configured to generate a first private key and corresponding first public key, generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 4, lines 25-30).

b. A storage medium coupled to the processor to store the first private key (column 2, lines 48-50).

c. A second private key that can be used when there is no access to the first private key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

d. Output the first public key and the second public key to a verifier device (column 4, lines 18-20).

e. Wherein the processor uses the stored first private key for authentication of the device prior to using the second private key (column 4, lines 15-23).

14. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

15. Referring to claim 56, Arthan teaches the second private key is removed from the user device upon transmission of the second private key (column 4, lines 30-32).

16. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among

multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

17. Claims 1 – 3, 5 – 9, 11 – 14, 16 – 24, 26 – 28, 51, 53 – 55, and 57 – 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan et al's US Patent 6,782,103 B1, and in view of Kurn et al's US Publication 2002/0071561 A1 and further in view of Hansmann et al's US Publication 2002/0018570 A1.

18. Referring to claims 1, 14 and 22, Arthan teaches:

f. Creating a first private key and corresponding public key (column 4, lines 25-30).

g. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 4, lines 25-30).

h. The second private key being used when the first private key is inaccessible (column 4, lines 25-32).

i. Transmitting the first public key and the second public key to a verifier device (column 4, lines 18-20).

j. Using the first private key for authentication prior to using the second private key (column 4, lines 15-23).

19. Arthan fails to teach outputting the private key such that it is not stored on the user device by transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

20. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

21. Referring to claims 2 and 23, Kurn teaches:

k. Creating at least two shares of the private key at the device (paragraph 89).

l. Outputting each share to a different entity (paragraph 89).

22. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

23. Referring to claims 3, 16, and 24, Arthan teaches using the second private key independent of the first private key for authentication (column 4, lines 20-23). Kurn teaches re-creating the private key using at least some shares of the plurality of shares (paragraphs 27 and 103). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

24. Referring to claims 5 and 17, Arthan teaches:

m. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 5, lines 12-14).

n. Outputting the third public key to the verifier (column 5, lines 12-14).

25. Referring to claim 6, Arthan teaches:

o. Outputting the third private key (column 4, lines 30-32).

p. Using the third private key for authentication (column 4, lines 20-23).

26. Kurn teaches:

q. Outputting the key as a plurality of shares such that it can be recreated (paragraph 89).

r. Recreating the private key using at least some of the plurality of shares (paragraph 27).

27. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

28. Referring to claim 7, Arthan teaches that the second private and public keys are created independently from the first private and public keys (column 4, lines 25-26).

29. Referring to claims 8 and 18, Arthan teaches:

s. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 5, lines 12-14).

t. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 4, lines 25-30).

u. Outputting the third and fourth public keys (column 4, lines 18-20).

30. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

31. Referring to claim 9, Arthan teaches:

v. Disabling use of the second private key for authentication (column 4, lines 20-23).

w. Using the third private key for authentication (column 4, lines 20-23).

x. Accessing the fourth private key (column 4, lines 20-23).

y. Using the fourth private key for authentication (column 4, lines 20-23).

32. Arthan fails to teach recreating the fourth private key. However, Kurn teaches using the shares to recreate the key (paragraph 27). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the

teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

33. Referring to claims 11, 19, and 26, Arthan discloses:

z. Receiving a first public key, wherein the first public key has a corresponding first private key stored in the user device (column 4, lines 18-23).

aa. Receiving a second public key, the second public key associated with the first public key (column 4, lines 18-20), wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to the first public key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

bb. Using the first public key for authentication (column 5, lines 12-14).

cc. Using the second public key for authentication if the first public key fails (column 5, lines 12-14).

34. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the

teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

35. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

36. Referring to claims 12, 20 and 27, Arthan teaches receiving a third public key from the device, the third public key associated with the second public key (column 5, lines 12-14), if the first public key fails and the second key results in successful authentication (column 4, lines 20-23).

37. Referring to claims 13, 21, and 28, Arthan teaches a third public key and a fourth public key from the device (column 5, lines 12-14), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 4, lines 20-26).

38. Referring to claim 51, Arthan teaches:

dd. A receiver configured to receive a first public key from a device and receiving a second public key from the device, wherein the first public key has a

corresponding first private key stored on the user device and the second public key associated with the first public key, wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to a first public key, wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 15-30).

ee. A storage medium coupled to the receiver configured to store the first and second public keys (column 4, lines 18-20).

ff. A processor coupled to the receiver and the storage medium, the processor configured to use the first public key for authentication, the processor configured to use the second public key for authentication if the first public key fails (column 4, lines 18-20).

39. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

40. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

41. Referring to claims 53 – 55, Arthan teaches the second private key is removed from the user device upon transmission of the second private key (column 4, lines 30-32).

42. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

43. Referring to claims 57, 61 and 65, Arthan teaches:

gg. Retrieving a second private key at a mobile user device that has no access to a first private key associated with the second private key (column 5, lines 12-14).

hh. Creating a third private key and a corresponding third public key (column 5, lines 12-14).

ii. Using the second private key for authentication before using the third private key (column 4, lines 20-23).

44. Arthan fails to teach recreating a key using at least some shares of a plurality of shares of the private key, or outputting the private key such that it is not stored on the user device. However, Kurn teaches that the protection key is split among multiple individuals, wherein the protection key can be recreated using seven shares of the private key (paragraphs 89-90) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

45. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been

obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

46. Referring to claim 58, 62 and 66, Kurn teaches recreating the second private key at a user device different from a user device that created the first private key and second private key (paragraph 94). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

47. Referring to claims 59, 63, and 67, Arthan teaches:

jj. Outputting the third private key while retaining the second private key (column 4, lines 30-32).

kk. Transmitting the third public key to the verifier device (column 4, lines 18-20).

48. Kurn teaches outputting the key as a plurality of shares such that it can be recreated (paragraphs 89-90). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn.

The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

49. Referring to claims 60, 64, and 68, Arthan teaches:

ll. Creating a fourth private key and a corresponding fourth public key (column 4, lines 25-30).

mm. Outputting the fourth private key while retaining the third private key (4, lines 30-32).

nn. Outputting the third and fourth public keys (column 4, lines 18-20).

50. Kurn teaches outputting the key as a plurality of shares such that it can be recreated (paragraphs 89-90). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

51. Claims 10 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan in view of Kurn in view of Hansmann as applied above, and further in view of Official Notice. Referring to claim 10, Arthan in view of Kurn in view of Hansmann discloses all the limitations of the parent claim. Arthan in view of Kurn in view of Hansmann does not explicitly disclose preventing retransmission of the second private key. However, Arthan teaches that the key is encrypted and stored securely (column 5,

lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

52. Referring to claim 15, Kurn teaches:

oo. Creating at least two shares of the second private key at the device (paragraph 89).

pp. Outputting each share to a different entity (paragraph 89).

53. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

54. Arthan in view of Kurn does not explicitly disclose subsequent outputting of the key is prevented. However, Arthan teaches that the key is encrypted and stored securely (column 5, lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Zecher whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Cordelia Zecher/
Examiner, Art Unit 2432